Nachtrag zur Dokumentation

ZoneAlarm-Sicherheitssoftware 7.1

Dieses Dokument behandelt neue Funktionen, die nicht in den lokalisierten Versionen des Benutzerhandbuchs berücksichtigt wurden. Klicken Sie unten in der Liste auf das gewünschte Element, um weitere Informationen anzuzeigen.

- **ZoneAlarm Identitätsschutz-Center**: Hilft Ihnen dabei, Identitätsdiebstahl vorzubeugen, zu erkennen und bei Bedarf zu beheben.
- **Spielemodus**: Unterdrückt vorübergehend alle Prüfungen, Produktaktualisierungen und Warnungen der ZoneAlarm-Sicherheitssoftware, so dass Sie auf Ihrem Computer mit weniger Unterbrechungen spielen können.
- **Spezieller Systemschutz durch OSFirewall**: Bestimmen Sie, welche Programme auf Ihrem Computer bestimmte Aktionen durchführen dürfen, beispielsweise Ihre Startseite in Internet Explorer ändern oder ActiveX-Steuerelemente installieren.
- **Optionen für die Virenprüfung**: Bietet die Möglichkeit, Dateien, die eine angegebene Größe überschreiten, zu umgehen und stellt eine erweiterte Malware-Datenbank bereit.
- **Systemspeicher prüfen**: Prüft den Arbeitsspeicher Ihres Computers.
- **Ausnahmeliste**: Bietet die Möglichkeit, eine Liste mit Elementen zu erstellen, die die Virenprüfung der ZoneAlarm-Sicherheitssoftware ignorieren soll.
- **Sicherheitsstufe**: Bietet einen Modus zum automatischen Lernen, durch den die Warnmeldungen minimiert werden, während die ZoneAlarm-Sicherheitssoftware Ihren Computer "kennenlernt".
- **Einstellen der Netzwerk-Sicherheitsoptionen**: Bietet die Möglichkeit Internetdatenverkehr über Internet Protocol 6 (IPv6) zuzulassen oder zu blockieren.
- **Korrekturen und Aktualisierungen der Dokumentation**

ZoneAlarm Identitätsschutz-Center

Auf Grund von E-Commerce, elektronischer Datenspeicherung und Massenmails sind Identitätsdiebstähle in den letzten Jahren immer häufiger aufgetreten. Hacker können

mit Hilfe von Malware Ihre persönlichen Daten online abfangen, während Diebe CDs und Laptops mit Kundendaten stehlen oder vertrauliche E-Mails (z. B. genehmigte Kreditkartenangebote) mit persönlichen Daten abfangen können.

Das ZoneAlarm Identitätsschutz-Center ist eine Website, die Ihnen dabei hilft, Identitätsdiebstahl vorzubeugen, zu erkennen und bei Bedarf zu beheben. Das Identitätsschutz-Center enthält Tipps zum Identitätsschutz sowie Ressourcen, um die Verwendung persönlicher Daten zu überwachen und einen Identitätsdiebstahl zu beheben.

Der Zugriff auf das Identitätsschutz-Center ist nur in ZoneAlarm Pro und ZoneAlarm Security Suite verfügbar.

So wechseln Sie zum Identitätsschutz-Center:

1. Wechseln Sie zu **Identitätsschutz|Grundeinstellungen**.
2. Klicken Sie im Bereich **Identitätsschutz-Center** auf **Zum ZoneAlarm Identitätsschutz-Center wechseln**.

Spielemodus

Der Spielemodus unterdrückt vorübergehend alle Prüfungen, Produktaktualisierungen und Warnungen der ZoneAlarm-Sicherheitssoftware, so dass Sie auf Ihrem Computer mit weniger Unterbrechungen spielen können. Mit Hilfe des Spielemodus können Sie alle Zugriffsanforderungen von Programmen vorübergehend zulassen oder ablehnen, so dass die ZoneAlarm-Sicherheitssoftware auf solche Anforderungen automatisch reagieren kann, ohne Warnungen anzuzeigen. Automatische Prüfungen und Produktaktualisierungen werden verschoben und erst durchgeführt, wenn Sie den Spielemodus deaktivieren. Der Spielemodus bleibt so lange aktiv, bis Sie ihn, die ZoneAlarm-Sicherheitssoftware oder Ihren Computer ausschalten.

Im Spielemodus werden alle Hinweise und Warnungen, in denen Sie aufgefordert werden, eine Entscheidung zu treffen, unterdrückt. Hierzu zählen Warnungen, die durch die Einstellung **Fragen** in der Programmliste verursacht werden, beispielsweise Zugriffswarnungen, die von einem Programm ausgelöst werden, das versucht eine E-Mail zu senden oder als Server zu fungieren. Hierzu zählen auch OSFirewall-Warnungen, in denen Sie aufgefordert werden, eine als ungewöhnlich oder verdächtig eingestufte Aktion zuzulassen oder abzulehnen. Die Einstellungen des Spielemodus übersteuern keine der Einstellungen für **Zulassen** oder Verweigern in Ihrer Programmliste. Wenn Sie die ZoneAlarm-Sicherheitssoftware konfiguriert haben, ein bestimmtes Programm immer zu sperren, wird dieses Programm auch gesperrt, wenn Sie den Spielemodus mit der Einstellung **Zulassen** aktivieren.

Durch die Verwendung des Spielemodus kann die Sicherheit Ihres Systems herabgesetzt werden. Wenn Sie angeben, dass alle Berechtigungsanforderungen zugelassen werden, wird das Risiko erhöht, dass ein gefährliches Programm auf Ihrem Computer Schaden anrichten oder auf Ihre Daten zugreifen kann.

Andererseits, wenn Sie alle Anforderungen ablehnen, können die Funktionen eines legitimen Programms unterbrochen werden. Deshalb sollten Sie den Spielemodus nur für die Dauer Ihres Spiels aktivieren.

So aktivieren Sie den Spielemodus:

1. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol, und wählen Sie **Spielemodus...** aus.
2. Klicken Sie im daraufhin angezeigten Dialogfeld zum Aktivieren des Spielemodus auf eine der folgenden Optionen:

   Alle Warnmeldungen mit „Zulassen" beantworten: Berechtigungsanforderungen werden gewährt.

   Alle Warnmeldungen mit „Ablehnen" beantworten: Berechtigungsanforderungen werden abgelehnt.
3. Lassen Sie das Dialogfeld zum Aktivieren des Spielemodus geöffnet, oder minimieren Sie es. Sie dürfen es jedoch nicht schließen. (Wenn Sie das Fenster schließen, wird der Spielemodus automatisch deaktiviert.)

   Während der Spielemodus aktiviert ist, zeigt die ZoneAlarm-Sicherheitssoftware ein spezielles Symbol, , in der Taskleiste an.

So deaktivieren Sie den Spielemodus:

Befolgen Sie eine der folgenden Anweisungen:

- Schließen Sie das Dialogfeld zum Aktivieren des Spielemodus, indem Sie auf **Abbrechen** oder rechts oben auf das Symbol zum Schließen (x) klicken.
- Klicken Sie im Dialogfeld zum Aktivieren des Spielemodus auf **Spielemodus stoppen**.
- Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol, und wählen Sie **Spielemodus stoppen** aus.

Beachten Sie, dass der Spielemodus automatisch deaktiviert wird, wenn Sie Ihren Computer oder die ZoneAlarm-Sicherheitssoftware ausschalten.

Spezieller Systemschutz durch OSFirewall

Der standardmäßig aktivierte OSFirewall-Schutz erkennt, wenn Programme versuchen, mit Ihrem Betriebssystem verdächtige Aktionen auf Ihrem Computer auszuführen. Sie können auch verschiedene Optionen des speziellen Systemschutzes durch OSFirewall konfigurieren, die bestimmen, welche Programme auf Ihrem Computer bestimmte Aktionen durchführen dürfen,

beispielsweise Ihre Startseite in Internet Explorer ändern oder ActiveX-Steuerelemente installieren.

Der spezielle Systemschutz durch OSFirewall kann einige der als mittelschwer eingestuften verdächtigen Verhaltensweisen verhindern, die im Anhang „Programmverhalten“ erläutert werden.

So konfigurieren Sie OSFirewall-Einstellungen:

1. Wählen Sie **Programmeinstellungen|Grundeinstellungen** aus.
2. Klicken Sie im Bereich **Programmeinstellungen** auf **Benutzerdefiniert**.
3. Wählen Sie im angezeigten Dialogfeld **Einstellungen für benutzerdefinierte Programmsteuerung** die Registerkarte **OSFirewall** aus.
4. Je nach Bedarf können Sie **OSFirewall aktivieren** aktivieren oder deaktivieren. (Hinweis: Um Optionen des speziellen Systemschutzes durch OSFirewall im nächsten Schritt aktivieren zu können, müssen Sie dieses Kontrollkästchen aktivieren.)
5. Konfigurieren Sie optional beliebige Optionen des speziellen Systemschutzes durch OSFirewall. Um auf eine Aktion in der Liste zuzugreifen, klicken Sie in das Feld **Status**, und wählen Sie **Zulassen**, **Verweigern**, **Fragen** oder **Programmeinstellungen verwenden** aus. Wenn Sie **Programmeinstellungen verwenden** auswählen, verwendet Zone Labs-Sicherheitssoftware entweder SmartDefense Advisor-Einstellungen oder Ihre manuellen Einstellungen.
6. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern und das Dialogfeld offen zu lassen, oder auf **OK**, um die Einstellungen zu speichern und das Dialogfeld zu schließen.

Optionen für die Virenprüfung

Sie können Ihre Virenprüfung so konfigurieren, dass alle Dateien, die eine bestimmte Größe (Standardeinstellung ist 8 MB) überschreiten, ignoriert werden. Durch diese Option, wird die Prüfzeit ohne erhöhtes Risiko verkürzt, da Virendateien normalerweise kleiner als 8 MB sind. Auch wenn große Dateien, die von der Prüfung ignoriert werden, möglicherweise Viren enthalten können, ist Ihr Computer weiterhin geschützt, wenn Sie Prüfen bei Zugriff aktiviert haben.

Sie können auch die erweiterte Datenbank aktivieren. Diese Datenbank enthält zusätzlich zu der Standardvirenliste eine umfassende Liste mit Malware. Allerdings kann sich manche in der Liste aufgeführte Malware auch in der Datenbank für Standard-Anti-Spyware befinden, sodass die eine oder andere potenzielle Malware doppelt geprüft wird. Auch die Malware-Liste der erweiterten Datenbank kann Programme enthalten, die als nützlich gelten.

So legen Sie Optionen für die Virenprüfung fest:

1. Wählen Sie **Antivirus/Anti-Spyware|Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**

   Das Dialogfeld **Erweiterte Optionen** wird angezeigt.

2. Wählen Sie unter **Virus-Verwaltung** die Option **Prüfungsoptionen** aus.
3. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Überspringen, wenn das Objekt größer ist als**.

   Wenn Sie dieses Kontrollkästchen aktiviert haben, geben Sie im Feld **MB** eine maximale Größe ein.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Erweiterte Datenbank aktivieren**, und klicken Sie dann auf **OK**.

Systemspeicher prüfen

Um den Systemspeicher zu prüfen, führen Sie die folgenden Schritte aus:

So prüfen Sie den Systemspeicher:

1. Wählen Sie **Antivirus/Anti-Spyware|Grundeinstellungen** aus.
2. Klicken Sie auf **Erweiterte Optionen**.

   Das Dialogfeld **Erweiterte Optionen** wird angezeigt.

3. Wählen Sie unter **Virus-Verwaltung** die Option **Ziele prüfen** aus.
4. Geben Sie an, welche Laufwerke, Ordner und Dateien geprüft werden sollen.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Boot-Sektoren aller lokalen Laufwerke prüfen**.
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Systemspeicher prüfen**, und klicken Sie dann auf **OK**.

Ausnahmeliste

Obwohl einige Programme, die von der erweiterten Datenbank als verdächtig eingestuft werden, Ihren Computer möglicherweise beschädigen oder Ihre Daten Hackerangriffen aussetzen können, gibt es auch viele nützliche Anwendungen, die bei einer Prüfung ebenfalls als Viren erkannt werden. Wenn Sie eine dieser Anwendungen verwenden, können Sie sie von den Antivirus-Prüfungen ausschließen, indem Sie sie der Ausnahmenliste hinzufügen. Sie können der Ausnahmenliste Programme hinzufügen, indem Sie mit der rechten Maustaste auf das Element in der Liste der Prüfungsergebnisse klicken und anschließend im Menü die Option Immer ignorieren auswählen.

Sobald sich Programme in der Ausnahmenliste befinden, werden sie bei Antivirus-Prüfungen nicht mehr erkannt. Wenn Sie der Ausnahmenliste versehentlich einen Virus hinzugefügt haben, können Sie ihn manuell entfernen.

So entfernen Sie Viren von der Ausnahmenliste:

1. Wählen Sie **Antivirus/Anti-Spyware|Grundeinstellungen** aus, und klicken Sie dann auf **Erweiterte Optionen**
2. Wählen Sie unter **Virus-Verwaltung** die Option **Ausnahmen** aus.
3. Wählen Sie im Bereich **Virenbehandlung - Ausnahmen** den Virus aus, den Sie entfernen möchten, und klicken Sie dann auf **Von Liste entfernen**.
4. Klicken Sie auf **OK**.

Sicherheitsstufe

Die ZoneAlarm-Sicherheitssoftware bietet zahlreiche Programmeinstellungs-methoden. Mithilfe der Basisprogrammeinstellungen können Sie Zugriffs- und Serverrechte für einzelne Programme festlegen. Mit den erweiterten Programm-einstellungen wird verhindert, dass Malware vertrauenswürdige Programme missbraucht. Über die Interaktionssteuerung für Anwendung werden Sie gewarnt, wenn ein Prozess versucht, einen anderen Prozess zu verwenden oder ein Programm ein anderes Programm zu starten versucht. Der OSFirewall-Schutz erkennt, wenn Programme versuchen, mit Ihrem Betriebssystem verdächtige Aktionen auf Ihrem Computer auszuführen.

Um die Anzahl der angezeigten Warnungen zu beschränken, können Sie die folgenden Funktionen verwenden:

- Wenn Sie die ZoneAlarm-Sicherheitssoftware mit Anti-virus einsetzen, verwenden Sie die Sicherheitsstufe **Autom. Lernen**. Mit **Autom. Lernen** erhalten Sie innerhalb der ersten 7 bis 21 Tage der Verwendung von ZoneAlarm-Sicherheitssoftware einen mittleren Schutz. Sobald ZoneAlarm-Sicherheitssoftware Ihren Computer kennt, werden die Programmeinstellungen auf **Max.** gesetzt.
- Wenn Sie von ZoneAlarm automatisch Vorschläge zu Programmeinstellungen erhalten möchten, verwenden Sie SmartDefense Advisor zusammen mit den Programmeinstellungen.

So legen Sie die Sicherheitsstufe für die Programmeinstellungen fest:

1. Wählen Sie **Programmeinstellungen|Grundeinstellungen** aus.

2. Klicken Sie im Bereich **Programmeinstellungen** auf den Schieberegler, und ziehen Sie ihn zur gewünschten Einstellung.

<table>
<tr><td>Max
(für Versionen mit Anti-virus)
Hoch
(für Versionen ohne Anti-virus)</td><td>Bei dieser Einstellung können viele Warnungen angezeigt werden.
◆ Programme benötigen Erlaubnis für Internetzugriff und Ausführung von Serverfunktionen.
◆ Die Überwachung von OSFirewall ist auf verdächtige Verhaltensweisen ausgerichtet.
◆ Die erweiterten Programmeinstellungen und die Interaktionssteuerung für Anwendung sind aktiviert.
◆ Die Komponenteneinstellungen sind standardmäßig deaktiviert.*</td></tr>
<tr><td>Auto
(für Versionen mit Anti-virus)</td><td>Durch diesen Modus wird die Anzahl der Warnungen minimiert.
◆ Diese Sicherheitsstufe ist für die ersten 7 bis 21 Tage weniger sicher.
◆ Netzwerk und OSFirewall überprüfen einige Programme.</td></tr>
<tr><td>Mittel
(für Versionen ohne Anti-virus)</td><td>Dies ist die Standardeinstellung.
◆ Programme benötigen Erlaubnis für Internetzugriff und Ausführung von Serverfunktionen.
◆ Die Überwachung von OSFirewall ist auf verdächtige Verhaltensweisen ausgerichtet.
◆ Die Komponenteneinstellungen sind standardmäßig deaktiviert.*</td></tr>
<tr><td>Min
(für Versionen mit Anti-virus)</td><td>◆ OSFirewall ist deaktiviert.
◆ Die Komponenteneinstellungen sind standardmäßig deaktiviert.*
◆ Servereinstellungen und Stealth-Modus sind verfügbar.</td></tr>
<tr><td>Niedrig
(für Versionen ohne Anti-virus)</td><td>◆ OSFirewall ist deaktiviert.
◆ Die Komponenteneinstellungen sind standardmäßig deaktiviert.*
◆ Servereinstellungen und Stealth-Modus sind nicht verfügbar.</td></tr>
</table>

Aus	Programmeinstellungen sind deaktiviert. ◆ Programme und Komponenten werden weder authentifiziert noch erlernt. ◆ Es werden keine Programmberechtigungen erzwungen. ◆ Allen Programmen werden Zugriffsrechte und Serverberechtigungen gewährt. ◆ Alle Programme können verdächtige Aktionen ausführen. ◆ Es werden keine Programmwarnungen angezeigt.

*Komponenteneinstellungen sind standardmäßig deaktiviert. Wenn Sie die Komponenteneinstellungen jedoch aktiviert haben, bleiben diese so lange aktiviert, bis die Programmeinstellungen auf Hoch, Mittel oder Niedrig eingestellt werden.

Einstellen der Netzwerk-Sicherheitsoptionen

Mit Hilfe der automatischen Netzwerkerkennung können Sie die Sichere Zone auf einfache Weise so konfigurieren, dass verbreitete Netzwerkaktivitäten wie die gemeinsame Nutzung von Dateien und Druckern nicht beeinträchtigt werden. Die ZoneAlarm-Sicherheitssoftware erkennt nur Netzwerke, mit denen Sie physisch verbunden sind. Netzwerke über Router oder virtuelle Netzwerkverbindungen werden nicht erkannt.

Sie können festlegen, ob die ZoneAlarm-Sicherheitssoftware die erkannten Netzwerke stillschweigend der Sicheren Zone hinzufügt, oder ob Sie jedes Mal gefragt werden sollen, ob ein neu erkanntes Netzwerk hinzugefügt oder abgelehnt werden soll.

So legen Sie Netzwerkeinstellungen fest:

1. Wählen Sie **Firewall|Grundeinstellungen** aus.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich **Netzwerkeinstellungen** Ihre Sicherheitseinstellungen aus.

Erkannte Netzwerke zur Sicheren Zone hinzufügen	Fügt der Sicheren Zone automatisch neue Netzwerke hinzu. Diese Einstellung bietet die geringste Sicherheit.
Erkannte Netzwerke von der Sicheren Zone ausschließen	Verhindert automatisch, dass der Sicheren Zone neue Netzwerke hinzugefügt werden und ordnet diese stattdessen der Internetzone zu. Diese Einstellung bietet die höchste Sicherheit.
Bei neu erkannten Netzwerken Zonenzuweisung erfragen	Die ZoneAlarm-Sicherheitssoftware zeigt eine „Neues Netzwerk"-Warnung oder den Netzwerk-Konfigurationsassistenten an, damit Sie die gewünschte Zone angeben können.

Neue ungeschützte Funknetzwerke (WEP oder WPA) automatisch in die Internetzone aufnehmen	Nimmt ungesicherte Funknetzwerke automatisch in die Internetzone auf, wodurch nicht autorisierter Zugriff auf Ihre Daten durch Dritte, die auf das Netzwerk zugreifen, verhindert wird.
IPv6-Netzwerk aktivieren	Datenverkehr über IPv6-Netzwerk zulassen, um auf Ihren Computer zuzugreifen.

Korrekturen und Aktualisierungen der Dokumentation

Die folgenden Abschnitte enthalten Korrekturen und Aktualisierungen, die nicht in die lokalisierten Versionen der Online-Hilfe und des Benutzerhandbuchs eingeschlossen wurden.

- „Spyware-Prüfungen“ auf Seite 9
- „Ausschließen von Spyware für Prüfungen“ auf Seite 9
- „Grundlegendes zu Ergebnissen von Virenprüfungen“ auf Seite 10
- „Komponenteneinstellungen“ auf Seite 10
- „Neues Verhalten der Option zum Speichern der Einstellung“ auf Seite 10
- „Namensänderung im Bildschirm „Firewall““ auf Seite 10
- „Neue Taskleistensymbole“ auf Seite 11

Spyware-Prüfungen

In der Dokumentation früherer Versionen der ZoneAlarm-Sicherheitssoftware steht, dass eine Spyware-Prüfung gestartet werden kann, indem eine Datei geöffnet oder mit der rechten Maustaste auf eine Datei geklickt und eine Prüfungsoption ausgewählt wird. Dies ist falsch.

Eine Viren-Prüfung kann auf zwei Arten gestartet werden:

- Sie können auf dem Bildschirm **Antivirus/Anti-Spyware** auf der Registerkarte **Grundeinstellungen** im Bereich **Anti-Spyware** auf **Auf Spyware prüfen** klicken.
- Sie können eine Systemprüfung planen, die einmal oder in regelmäßigen Intervallen ausgeführt wird. (Weitere Informationen zum Konfigurieren dieser Option finden Sie in der entsprechenden Online-Hilfe.)

Ausschließen von Spyware für Prüfungen

In früheren Versionen der Dokumentation fehlen in den Anweisungen zum Ausschließen spezifischer Programme von Prüfungen einige Details. Es folgt der korrigierte Text:

Obwohl einige Spyware-Programme möglicherweise Ihren Computer beschädigen oder Ihre Daten Hackerangriffen aussetzen können, gibt es auch viele nützliche Anwendungen, die bei einer Prüfung ebenfalls als Spyware erkannt werden. Wenn Sie eine dieser Anwendungen verwenden, beispielsweise Spracherkennungs-

Software, können Sie sie von den Spyware-Prüfungen ausschließen, indem Sie sie der Ausnahmenliste hinzufügen. Sie können Spyware der Ausnahmenliste hinzufügen, indem Sie mit der rechten Maustaste auf das Element in der Liste der Prüfungsergebnisse klicken und anschließend im Menü die Option Immer ignorieren auswählen.

Grundlegendes zu Ergebnissen von Virenprüfungen

Das Dialogfeld **Prüfungsergebnisse**, das nach Viren- und Spyware-Prüfungen angezeigt wird, verfügt nun über einen Bereich mit Details. Nach Spyware-Prüfungen enthält der Bereich **Details** eine Liste der vollständigen Pfade aller Spyware-Spuren (z. B. Registrierungsschlüssel, Cookies usw.). Diese Informationen können für erfahrene Benutzer hilfreich sein, die die Spyware-Programme verfolgen möchten, die von der ZoneAlarm-Sicherheitssoftware nicht automatisch behandelt werden. Bei Virenprüfungen bleibt der Bereich für Details leer.

Komponenteneinstellungen

Die Dokumentation wurde aktualisiert, so dass die Interaktion zwischen Programm- und Komponenteneinstellungen nun genauer beschrieben wird. Es folgt der aktualisierte Text:

Unabhängig von der Einstellung für die Programmeinstellungen sind die Komponenteneinstellungen standardmäßig deaktiviert. Wenn Sie die Sicherheitsstufe für die Programmeinstellungen ändern, werden die Komponenteneinstellungen nicht automatisch aktiviert. Wenn Sie die Komponenteneinstellungen jedoch aktivieren, bleiben diese so lange aktiviert, bis die Programmeinstellungen auf **Hoch**, **Mittel** oder **Niedrig** eingestellt werden.

Neues Verhalten der Option zum Speichern der Einstellung

Das Kontrollkästchen **Diese Einstellung speichern** für Programmwarnungen verhält sich in Version 6.5 anders als in früheren Versionen. Es folgt die neue Beschreibung:

Solange SmartDefense Advisor auf **Auto** eingestellt ist, gibt die Zone Labs-Sicherheitssoftware nur Programmwarnungen aus, wenn keine automatische Einstellung verfügbar ist. Wenn Sie die Option **Diese Einstellung speichern** in einer Programmwarnung aktivieren, wenn der Programmzugriff gestattet oder verweigert wird, behält die Zone Labs-Sicherheitssoftware Ihre Einstellung nur bei, wenn SmartDefense Advisor über keine andere Einstellung verfügt, oder Sie die Einstellung manuell auf der Registerkarte **Programme** ändern. Wenn Sie **Diese Einstellung speichern** nicht aktivieren, gibt die Zone Labs-Sicherheitssoftware eine weitere Programmwarnung aus, wenn das Programm dieselbe Aktion ein weiteres Mal versucht.

Namensänderung im Bildschirm „Firewall"

Der Name einer Einstellung der Sicherheit für die Internetzone und der Sicherheit für die Sichere Zone, die sich im Bildschirm **Firewall** auf der Registerkarte **Grundeinstellungen** befinden, wurde geändert. Die Einstellung **Niedrig** wurde in **Aus** umbenannt.

Neue Taskleistensymbole

Die Version 6.5 enthält folgende neue Taskleistensymbole:

Symbol	Beschreibung
	Die ZoneAlarm-Sicherheitssoftware führt eine Viren- und/oder Spyware-Prüfung durch. Details zu Viren- und Spyware-Prüfungen finden Sie in der entsprechenden Online-Hilfe sowie in den Abschnitten zu Spyware unter „Korrekturen und Aktualisierungen der Dokumentation“ auf Seite 9 in diesem Dokument. Wenn dieses Symbol angezeigt wird, können Sie darauf klicken und **Prüfung anzeigen** auswählen, um das Dialogfeld **Prüfstatus** aufzurufen.
	Der Spielemodus ist aktiviert und die ZoneAlarm-Sicherheitssoftware unterdrückt Aktualisierungen, Prüfungen und die meisten Warnungen. Details zum Spielemodus finden Sie unter „Spielemodus“ auf Seite 2.
	Die ZoneAlarm-Sicherheitssoftware erhält eine Aktualisierung, beispielsweise neue Viren- oder Spyware-Definitionen.